### Algorithm 1 Salsa20

### Algorithm Attack of Require: New 2 Block Counter Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Require: New 2 Block Counter and Algorithm Attack of Requirement and Algorithm Attack o Require:InitialMatrix(

Require: Réquire: T
The streims vipble estatique de la spontation attacks
out a incorpsion equipment of the street of the s input a most siance one output bit key C add: ) and a 64-bit nonce and products a stong that the source of the state of the

block closuser of the second fill the strain of four termines and nonce.

Abstract — Wanther than a second the strain of four termines and nonce.

Abstract — Wanther than a second the strain of the ization, duplicational and migraty at these sines are motival tablector the 11 softwago implementation (see a favoring is interest that the perfect of the p with the control of t celled possible by the control of the manual conference are a control of the cont

even rounds. All polition has the continued in proceeding of the continued in the continued implementation of Fault sample and perspection of Fault sample and perspection high performance and Algorithm his complementation using coGhachaeutsteanagan as than which promise there เมื่อใช้เลี้ย์คุกรีเบplication (dual/triple modular redundant), and parity checking may not be applicable. Then, we study the

Ensulation Round \*/ th block is the original straight of the corresponding to the correspond [19] A. Penbaoui, J. M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria, Injection of transfer and A. Tria, Injection of transfer and A. Tria, feast Fitz of cauty and bloos on Fault in the Half Subjection agnetic pulses the IA
13 and plates of any ferrore in Cryptography (F C 2012) 2012, and plates of any ferrore in Cryptography (F C 2012) 2012, and plates of any ferrore in Cryptography (F C 2012) 2012, and plates of any ferrore in Cryptography (F C 2012) 2013, and Encrenaz, in the Cryptography of C 2012 2013, and Encrenaz, in the Cryptography (F C 2012) 2013, and Encrenaze in Crypt

Returnal L. B. Glerich Tannosera whether retical model to break cryptographics benefit the first of the second and base cryptography are of soldship and plants and the second soldship and th ShaMmanilla be the well to keep the grave of the rableyed strainer merkion actual proposed and offerent fault model "Constructive Side-Channel Analysis and Secure estan (COSA); number of cipherexture Side-Channel Analysis and Secure estan (COSA); number of cipherexture Blenec and Secure 270 applied, an optical fault

2 0 [33], [34] have been analyzed using fault injection attack. addle IETF version [3] of ChaCha takes a 32-bit block counter C = ( c<sub>0</sub>) all 196 All GONGLIND WINGS REPLICATION AND CHACHA, 1037 1037 X15 = n2. Furthermore, 4, 128-bit key is out of scope in the IETF version. 1036 Weef 666 This line there does abgarrething proposels are known and ChaCha. 10SchaCha is a variant of Salsa20, and we show how it the differs

1033

#### Algorithm 1 Salsa20

# A. Salts a Linjection Attack Original of the Manual Action Attack

Require: ey K, Block Counter C, and Nance N

The stream with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 3P Distriction of 128input axis birther with the properties of 128input axis bit keyYK8  $= \lambda (k_0, k_1, k_2, k_3)$  and a 64-bit nonce  $N = (n_0, n_1)$ , and produces assence the management by the string and produces assence of the string and produces as the string and produces as the string and produced as the string as the str th block is the one of the state of the control of

(x), x surguysi aur x aur ministry the phocycounter and nonce that food. In one of the k2 instructions that add words of 2 8 thek initial many x and x

Algorithm and production of infinitely suream change, i.e.,

Algorithm in the proposed with the problem of the p tures: T) Routs has this item to make the property and from the contract of th in, which we consider the contents of the content o transforme than as redam applicat, which ich means and artizaddinan

tarioforme that a several policies, which it is nearest that the project for settle and several policies, which is the project for settle and the project for the project for settle and the project for the bead based from the separation of Chacha. head based from the separation of chacha. The separation is the separation of chacha. high performance and Algorithm his hows the implementation using contact mensure and specific an monthships duplication (dual/triple modular redundant), and parity checking may not be applicable. Then, we study the

for 8: In things to such the C, Nand Nonce izt &dd the ystriam Pound \*/

feasibility of salvariable acousticine countering a sure in the IA-32 and Intel 14 and ARM nonlinearing mil (x113012, x13)

1201 Referred Pendadily of Heyderian Berosson, and E. Erlerenaz, 214)

1201 Referred Pendadily of Heyderian Berosson, and E. Erlerenaz, 214)

1201 Referred Pendadily of Heyderian Berosson, and E. Erlerenaz, 214

1201 Referred Pendadily of Table 1 are on a 32-bit 21 and 22 microcontroller, in 1781 E. 1 are on a 12-bit 21 and 22 microcontroller, and 22 microcontroller, and 23 microcontroller, and 24 microcontroller, and 25 micr

Z (microcontroller, in TABLE 1 p. 17 18 metricales model to break cryptographiceschicus de Sparagon and antique sparagon hardware that their attack applies to implement a their attack applies to implement a transfer that their attack applies to Shamman the state of the state ble the family printed and the property of the madel Conserviver Side Change and State Sound From Price and Language of a la faction of the control of th

of the property of the control of th on Alexandra enum included the confusion and side channel attack on a second confusion and side channel attack on a second confusion and side channel attack on a second confusion and side confusion and s

The values in the particular property was another the second content of the particular p demonstrated that the property of the property clock signal was proported by Bather, hpet 2 als. [21], Korak and

Hoeter the state of the state o a singly of the second of the

function A in the machine large A in Aallivousilusathereinidatisme sandinainsi saassa sia ann daeas acida, 1037 Innertible Futhermontre the Sit bey adouble come in the VETE version. 1036 Weel FRETHRE the the abeartething proposet and and ChaCha. 10SchaCha is a variant of Salsa20, and we show how it the differs

Salsa20

# Require: Key K, Block Counter C, and Nonce N Increase in the state of RevuireInitialMatrixMteCQNand Nonce N input aiden keinen stellen ste Require: Ikinulliple instructions in supering in the continue of the continue dependent of the word with the keystreams, message authorization code, and the word with the keystreams, message authorization code, of the word with the keystreams, message authorization code, of the word with the keystreams, message authorization code, of the word with the keystreams, message authorization code, of the word with the word with the word substantial and the word with the word with the word substantial and the word with the word substantial and the word with central processing and the process of the process o

1034 1033

coldie Programmes and constant distance rotations. Amountained Furthernous and 2014 sealisulated, sone in the W Fancision. The programmes and constant distance rotations. Amountained function (dual triple modular redundant), and constant distance rotations and constant distance rotations and constant distance rotations and constant distance rotations. parity checking may not be applicable. hen, we study the Charles is a variant of Salsa20, and we show how it the differs

# alsalgorithaulta Injection Attack of Require: Yes Rock Counter Cant Non Contact of Republic R

Algorithm 1 Salsa20

Require: lo outr radio or 128
The streing and one output.

Require: Require: Institution to radio or 128
Require: Re bit key of add:
and a 64-bit nonce
and produces a content of the spinor input a input

Abgorithmattiple vällestine wandsalle the Revistrealit changed i.e.,

Adgorathmenting value but warmen in the Reystream charge, i.e., r Require: from the points tructions of the Reystream charge, i.e., r Require: from the points tructions of the Reystream charge, i.e., r Require: from the rest of the Reystream charge in the Re is, whethere the state of the s

head based nonthe instrument property of the control of the contro high performance pant Algorithm his hows the implementation estings coGhachaeuther aga a sail sho caichte ann an air an lenving than the first of the state of the s parity checking may not be applicable. Then, we study

shaMinanien are the control of the c ble to spring the ble to a charge of the proposed or different fault model Conjection of the Land State of Singly Print an small number of ciphigrexis. Blomer and States 47 applied an optical fault of ciprogreeks. Blomer and Senert and supplied an optical fault in a ciprogreeks of the c on Alexanded entities in \$100 and to the total or handproposed augustifolomical, differentials faint sinjection and street hanne battack oip s gate to 556346684 6473465477617 3 the addition result of

througher with a separation and hard range with a range can be and the state of the state o Purification of the content of the c

against ledge at a more partially and the consumer of the ledge at the 2.0 d 38 1.1 [34] before been sabaly sed asing Pauls infection attack.

alle och action of the second 1036 Tribl Furthernstne a 128-bit key is lowled stops in the 11272 version. a variant of Salsa20, and we show how it the differs

1035 1034

1033

Algorithm 1 Salsa20

from Salsa20.

```
require: ey , loc countered orgentered and orgentered and a Z
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                <del>a</del>nd Cha
              A. Salsazoi Andhach
                                                                                                                                                                                                , Block Counter C, and Nonce \Lambda
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           RequbirerKietyialCoutnicerXC, and Nonce N
                                                    Require Key
                                                 hastrewayment of the partite of the perturbation of the contraction of the second of the contraction of the second of the contraction of the contr
Sequential principles and a control of the control 
               Recording Matricon E. and
              bit Ey\sigma adk_0, k_1, k_2, k_3 and a 64-bit nowhice n_0, n_1 ,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Ensigne: Column & Roundy)*{/
               and produced to sepreministic of the land of the sepreministic of the se
            high penindal management in the property of the penind of the penind of the peninde counter that the penind of the
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            The keystream a 138 calculated as out of scopand, the version of the control of t
               anly additions, exclusive-or, and constant-distance rotation (qual/triple modu
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           1036
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   wastadny ishe variant of Salsa20, and we show how it the diffe
               parity chec ing may not be applicable. hen,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             1034
```

1033

### Algorithm 1 Salsa20

Require:InitialMatrix( n-r , and N nc

## Algorithm Attack of Require: Key of Rock Counter of Require: Key of Require: K

input a profile process of the proce impering and a second process of the second process of the second performance of the second perf software oin plantage of the conjustification of the c quarter sound functions in proceeding to propagate from the form the factors of the control of t transformeding as a second uproject, which is a 49 tandardization in project for sadamusphers, the control of t

of Salsazu wid word Cossinerain such by the Average of Salsazu head based no null a marting head separation and the head based no null and the head based null and the head implantation of the management of the state high performance and Algorithm his constitution and the performance of any and the performance of the perfor coGharmeuscreentswarts and another transfer in the continue of the **Wordi Zartin**, Suplication (dual/triple modular redundant), and parity checking may not be applicable. Then, we study the

Esorth AST to a Saut firection attacks Records P (P) Records P) Records P (P) Records P (P

cryptographics of the property of the property

ain NESSEE IN 5365 Joseph 32-250 Carrior Ban addition, preplit of the confidence of To code in Fire spanish 2. The But on the Square spanish that is the spanish of the But of the Square spanish of the But of the Square and multiply named to the Square spanish that is the square spanis Langley designed a strong chick promote the proposed strong to the control of the d Hoener nightal was producted to the production of the first status of the first stat 2/0°[33] alate been all alyzed using fault in jection attacked addle de THP version [3] poll ChaCharakbs a 32-bir block counter & =a co

nd

nd

ari y

CORRESTED AND THE REST OF THE CHARLES AND THE Furthermoreya 128 bit keyers out of scaperin the 129th version.

1036 We of Engline here also intended in proposely and chacha. 10SchaCha is a variant of Salsa20, and we show how it the differs